Invitation to Bid

LSUHSC-SHREVEPORT

LSU Health Sciences Center

VENDOR NO. :
SOLICITATION : 005452
OPENING DATE : 03/26/2010

BIDS WILL BE PUBLICLY OPENED:

March 26,2010 02:00 PM

Return Bid in Envelope/Labels Provided to:
Purchasing Department
PO Box 33932
Shreveport LA 71130

BUYER : Wilson, Judy
BUYER PHONE : 318/675-5290
DATE ISSUED : 03/09/2010
REQ. NO : 0043881
FISCAL YEAR : 2010

Wireless Local Area Network

INSTRUCTIONS TO BIDDERS

1. READ THE ENTIRE BID, INCLUDING ALL TERMS AND CONDITIONS AND SPECIFICATIONS.
2. FILL IN ALL BLANK SPACES.
3. ALL BID PRICES MUST BE TYPED OR WRITTEN IN INK. ANY CORRECTIONS, ERASURES OR OTHER FORMS OF ALTERATION TO UNIT PRICES SHOULD BE INITIALIZED BY THE BIDDER.
4. BID PRICES SHALL INCLUDE DELIVERY OF ALL ITEMS F.O.B. DESTINATION OR AS OTHERWISE PROVIDED. BIDS CONTAINING "PAYMENT IN ADVANCE" OR "C.O.D." REQUIREMENTS MAY BE REJECTED. PAYMENT IS TO BE MADE WITHIN 30 DAYS AFTER RECEIPT OF PROPERLY EXECUTED INVOICE OR DELIVERY, WHICHEVER IS LATER.
5. SPECIFY YOUR PAYMENT TERMS: _____ . CASH DISCOUNTS FOR LESS THAN 30 DAYS OR LESS THAN 1% WILL BE ACCEPTED, BUT WILL NOT BE CONSIDERED IN DETERMINING AWARDS

BY SIGNING THIS BID, THE BIDDER CERTIFIES:

* THAT NEITHER THIS BUSINESS ENTITY NOR ANY OF ITS EMPLOYEES OR SUBCONTRACTORS IS CURRENTLY LISTED AS EXCLUDED OR SANCTIONED BY EITHER THE DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE OF INSPECTOR GENERAL (OIG) OR THE GENERAL SERVICES ADMINISTRATION (GSA).
* THAT IF THIS BUSINESS ENTITY OR ANY OF ITS EMPLOYEES OR SUBCONTRACTORS APPEAR ON EITHER LISTING, MY BID WILL BE REJECTED.
* THAT IF AT ANY TIME DURING THE TERM OF THE CONTRACT AWARDED AS A RESULT OF THIS INVITATION TO BID, THIS ENTITY OR ANY OF ITS EMPLOYEES OR SUBCONTRACTORS APPEARS ON EITHER LISTING, MY COMPANY WILL NOTIFY THE CONTRACTING AGENCY, AND THE CONTRACT WILL BE TERMINATED. THE CONTRACTING AGENCY WILL NOT BE LIABLE FOR ANY DAMAGES RESULTING FROM SAID TERMINATION.

THE BIDDER FURTHER CERTIFIES:

* COMPLIANCE WITH ALL INSTRUCTIONS TO BIDDERS, TERMS, CONDITIONS, AND SPECIFICATIONS.
* THIS BID IS MADE WITHOUT COLLUSION OR FRAUD.
* THAT ALL TAXES DULY ASSESSED BY THE STATE OF LOUISIANA AND IT'S SUBDIVISIONS, INCLUDING FRANCHISE TAXES, PRIVILEGE TAXES, SALES TAXES AND ALL OTHER TAXES FOR WHICH THE FIRM IS LIABLE HAVE BEEN PAID.
* THAT IF MY BID IS ACCEPTED WITHIN _____ DAYS FROM BID CLOSING TIME, MY FIRM WILL FURNISH ANY OR ALL OF THE ITEMS (OR SECTIONS) AT THE PRICE OPPOSITE EACH ITEM (OR SECTION).
* DELIVERY WILL BE MADE WITHIN _____ DAYS AFTER RECEIPT OF ORDER.

VENDOR PHONE NUMBER: FAX NUMBER:	TITLE	DATE
SIGNATURE OF AUTHORIZED BIDDER (MUST BE SIGNED)	NAME OF BIDDER (TYPED OR PRINTED)	

STANDARD TERMS & CONDITIONS	Page 2 of 6
NUMBER : 005452 OPEN DATE : 03/26/2010 TIME: 02:00 PM	BIDDER:

6. DESIRED DELIVERY: 10 DAYS ARO, UNLESS SPECIFIED ELSEWHERE
7. TO ASSURE CONSIDERATION, ALL BIDS SHOULD BE SUBMITTED IN THE SPECIAL ENVELOPE, OR USE BID LABEL IF FURNISHED FOR THAT PURPOSE. IN THE EVENT YOUR BID CONTAINS BULKY SUBJECT MATERIAL, THE SPECIAL BID ENVELOPE SHOULD BE FIRMLY AFFIXED TO THE MAILING ENVELOPE.
8. BIDS SUBMITTED ARE SUBJECT TO PROVISIONS OF THE LAWS OF THE STATE OF LOUISIANA INCLUDING BUT NOT LIMITED TO L.R.S. 39:1551-1736; PURCHASING RULES AND REGULATIONS; EXECUTIVE ORDERS; STANDARD TERMS AND CONDITIONS;SPECIAL CONDITIONS; AND SPECIFICATIONS LISTED IN THIS SOLICITATION.
9. IMPORTANT: THIS BID IS TO BE MANUALLY SIGNED IN INK BY A PERSON AUTHORIZED TO BIND THE VENDOR (SEE NO.31).
10. INQUIRIES: ADDRESS ALL INQUIRIES AND CORRESPONDENCE TO THE BUYER AT THE PHONE NUMBER AND ADDRESS SHOWN ABOVE.
11. BID FORMS: ALL WRITTEN BIDS, UNLESS OTHERWISE PROVIDED FOR, SHOULD BE SUBMITTED ON, AND IN ACCORDANCE WITH FORMS PROVIDED, PROPERLY SIGNED (SEE #31). BIDS MUST BE RECEIVED AT THE ADDRESS SPECIFIED IN THE SOLICITATION PRIOR TO BID OPENING TIME IN ORDER TO BE CONSIDERED.
12. STANDARDS OR QUALITY. ANY PRODUCT OR SERVICE BID SHALL CONFORM TO ALL APPLICABLE FEDERAL AND STATE LAWS AND REGULATIONS AND THE SPECIFICATIONS CONTAINED IN THE SOLICITATION. UNLESS OTHERWISE SPECIFIED IN THE SOLICITATION, ANY MANUFACTURER'S NAME, TRADE NAME, BRAND NAME, OR CATALOG NUMBER USED IN THE SPECIFICATION IS FOR THE PURPOSE OF DESCRIBING THE STANDARD OF QUALITY, PERFORMANCE, AND CHARACTERISTICS DESIRED AND IS NOT INTENDED TO LIMIT OR RESTRICT COMPETITION. BIDDER MUST SPECIFY THE BRAND AND MODEL NUMBER OF THE PRODUCT OFFERED IN HIS/HER BID. BIDS NOT SPECIFYING BRAND AND MODEL NUMBER SHALL BE CONSIDERED AS OFFERING THE EXACT PRODUCTS SPECIFIED IN THE SOLICITATION.
13. DESCRIPTIVE INFORMATION. BIDDERS PROPOSING AN EQUIVALENT BRAND OR MODEL SHOULD SUBMIT WITH THE BID, INFORMATION (SUCH AS ILLUSTRATIONS, DESCRIPTIVE LITERATURE, TECHNICAL DATA) SUFFICIENT FOR LSUHSC TO EVALUATE QUALITY, SUITABILITY, AND COMPLIANCE WITH THE SPECIFICATIONS IN THE SOLICITATION. FAILURE TO SUBMIT DESCRIPTIVE INFORMATION MAY CAUSE BID TO BE REJECTED. ANY CHANGE MADE TO A MANUFACTURER'S PUBLISHED SPECIFICATION SUBMITTED FOR A PRODUCT SHALL BE VERIFIABLE BY THE MANUFACTURER. IF ITEM(S) BID DO NOT FULLY COMPLY WITH SPECIFICATIONS (INCLUDING BRAND AND/OR PRODUCT NUMBER), BIDDER MUST STATE IN WHAT RESPECT ITEMS(S) DEVIATE. FAILURE TO NOTE EXCEPTIONS ON THE BID FORM WILL NOT RELIEVE THE SUCCESSFU BIDDER(S) FROM SUPPLYING THE ACTUAL PRODUCTS REQUESTED.
14. BID OPENING. BIDDERS MAY ATTEND THE BID OPENING, BUT NO INFORMATION OR OPINIONS CONCERNING THE ULTIMATE CONTRACT AWARD WILL BE GIVEN AT THE BID OPENING OR DURING THE EVALUATION PROCESS. BIDS MAY BE EXAMINED WITHIN 72 HOURS AFTER BID OPENING. INFORMATION PERTAINING TO COMPLETED FILES MAY BE SECURED BY VISITING LSUHSC DURING NORMAL WORKING HOURS. WRITTEN BID TABULATIONS WILL NOT BE FURNISHED.
15. AWARDS. AWARD WILL BE MADE TO THE LOWEST RESPONSIBLE AND RESPONSIVE BIDDER. LSUHSC RESERVES THE RIGHT TO AWARD ITEMS SEPARATELY, GROUP, OR IN TOTAL, AND TO REJECT ANY OR ALL BIDS AND WAIVE ANY INFORMALITIES.
16. PRICES. UNLESS OTHERWISE SPECIFIED BY LSUHSC IN THE SOLICITATION, BID PRICES MUST BE COMPLETE, INCLUDING TRANSPORTATION PREPAID BY BIDDER TO DESTINATION AND FIRM FOR ACCEPTANCE FOR A MINIMUM OF 30 DAYS. IF ACCEPTED, PRICES MUST BE FIRM FOR THE CONTRACTUAL PERIOD. BIDS OTHER THAN F.O.B. DESTINATION MAY BE REJECTED. PRICES SHOULD BE QUOTED IN THE UNIT (EACH,

STANDARD TERMS & CONDITIONS	Page 3 of 6
NUMBER : 005452 OPEN DATE : 03/26/2010 TIME: 02:00 PM	BIDDER:

BOX, CASE, ETC.) AS SPECIFIED IN THE SOLICITATION.

17. DELIVERIES. BIDS MAY BE REJECTED IF THE DELIVERY TIME INDICATED IS LONGER THAN THAT SPECIFIED IN THE SOLICITATION.

18. TAXES. VENDOR IS RESPONSIBLE FOR INCLUDING ALL APPLICABLE TAXES IN THE BID PRICE. LSUHSC AGENCIES ARE EXEMPT FROM ALL STATE AND LOCAL SALES AND USE TAXES.

19. NEW PRODUCTS. UNLESS SPECIFICALLY CALLED FOR IN THE SOLICITATION, ALL PRODUCTS FOR PURCHASE MUST BE NEW, NEVER PREVIOUSLY USED, AND THE CURRENT MODEL AND/OR PACKAGING. NO REMANUFACTURED, DEMONSTRATOR, USED OR IRREGULAR PRODUCT WILL BE CONSIDERED FOR PURCHASE UNLESS OTHERWISE SPECIFIED IN THE SOLICITATION. THE MANUFACTURER'S STANDARD WARRANTY WILL APPLY UNLESS OTHERWISE SPECIFIED IN THE SOLICITATION.

20. CONTRACT CANCELLATION. THE STATE OF LOUISIANA HAS THE RIGHT TO CANCEL ANY CONTRACT, IN ACCORDANCE WITH PURCHASING RULES AND REGULATIONS, FOR CAUSE INCLUDING BUT NOT LIMITED TO THE FOLLOWING: (1) FAILURE TO DELIVER WITHIN THE TIME SPECIFIED IN THE CONTRACT; (2) FAILURE OF THE PRODUCT OR SERVICE TO MEET SPECIFICATIONS, CONFORM TO SAMPLE QUALITY OR TO BE DELIVERED IN GOOD CONDITION; (3) MISREPRESENTATION BY THE CONTRACTOR; (4) FRAUD, COLLUSION CONSPIRACY OR OTHER UNLAWFUL MEANS OF OBTAINING ANY CONTRACT WITH THE STATE; (5) CONFLICT OF CONTRACT PROVISIONS WITH CONSTITUTIONAL OR STATUTORY PROVISIONS OF STATE OR FEDERAL LAW; (6) ANY OTHER BREACH OF CONTRACT.

21. DEFAULT OF CONTRACT. FAILURE TO DELIVER WITHIN THE TIME SPECIFIED IN THE BID WILL CONSTITUTE A DEFAULT AND MAY CAUSE CANCELLATION OF THE CONTRACT. WHERE THE UNIVERSITY HAS DETERMINED THE CONTRACTOR TO BE IN DEFAULT, THE UNIVERSITY RESERVES THE RIGHT TO PURCHASE AN OR ALL PRODUCTS OR SERVICES COVERED BY THE CONTRACT ON THE OPEN MARKET AND TO CHARGE THE CONTRACTOR WITH COST IN EXCESS OF THE CONTRACT PRICE. UNTIL SUCH ASSESSED CHARGES HAVE BEEN PAID, NO SUBSEQUENT BID FROM THE DEFAULTING CONTRACTOR WILL BE CONSIDERED.

22. ORDER OF PRIORITY. IN THE EVENT THERE IS A CONFLICT BETWEEN THE INSTRUCTIONS TO BIDDERS OR STANDARD CONDITIONS AND THE SPEICAL CONDITIONS, THE SPECIAL CONDITIONS SHALL GOVERN.

23. APPLICABLE LAW. ALL CONTRACTS SHALL BE CONSTRUED IN ACCORDANCE WITH AND GOVERNED BY THE LAWS OF THE STATE OF LOUISIANA.

24. EQUAL OPPORTUNITY. BY SUBMITTING AND SIGNING THIS BID, BIDDER AGREES THAT HE/SHE WILL NOT DISCRIMINATE IN THE RENDERING OF SERVICES TO AND/OR EMPLOYMENT OF INDIVIDUALS BECAUSE OF RACE, COLOR, RELIGION, SEX, AGE, NATIONAL ORIGIN, HANDICAP, DISABILITY, VETERAN STATUS, OR A OTHER NON-MERIT FACTOR.

25. SPECIAL ACCOMMODATIONS. ANY "QUALIFIED INDIVIDUAL WITH DISABILITY" AS DEFINED BY THE AMERICANS WITH DISABILITIES ACT WHO HAS SUBMITTED A BID AND DESIRES TO ATTEND THE BID OPENING, MUST NOTIFY THIS OFFICE IN WRITING NOT LATER THAN SEVEN DAYS PRIOR TO THE BID OPENING DATE OF THEIR NEED FOR SPECIAL ACCOMMODATIONS. IF THE REQUEST CANNOT BE REASONABLY PROVIDED, THE INDIVIDUAL WILL BE INFORMED PRIOR TO THE BID OPENING.

26. IDEMNITY. CONTRACTOR AGREES, UPON RECEIPT OF WRITTEN NOTICE OF A CLAIM OR ACTION, TO DEFEND THE CLAIM OR ACTION, OR TAKE OTHER APPROPRIATE MEASURE, TO IDEMNIFY, AND HOLD HARMLESS, LSUHSC, ITS OFFICERS, ITS AGENTS AND ITS EMPLOYEES FROM AND AGAINST ALL CLAIMS AND ACTIONS FOR BODILY INJURY, DEATH OR PROPERTY DAMAGES CAUSED BY THE FAULT OF THE CONTRACTOR,

STANDARD TERMS & CONDITIONS	Page 4 of 6
NUMBER : 005452 OPEN DATE : 03/26/2010 TIME: 02:00 PM	BIDDER:

OFFICERS, ITS AGENTS, OR ITS EMPLOYEES. CONTRACTOR IS OBLIGATED TO INDEMNIFY ONLY TO THE EXTENT OF THE FAULT OF THE CONTRACTOR, ITS OFFICERS, ITS AGENTS, OR ITS EMPLOYEES. HOWEVER, THE CONTRACTOR SHALL HAVE NO OBLIGATION AS SET FORTH ABOVE WITH RESPECT TO ANY CLAIM OR ACTION FROM BODILY INJURY, DEATH OR PROPERTY DAMAGES ARISING OUT OF THE FAULT OF THE UNIVERSITY, ITS OFFICERS, ITS AGENTS OR ITS EMPLOYEES.

27. INTERPRETATION OF DOCUMENT: ANY INTERPRETATION OF THE BID OR QUOTATION DOCUMENT WILL ONLY BE MADE BY AN ADDENDUM ISSUED IN WRITING BY THE PURCHASING DEPARTMENT. SUCH ADDENDUM WILL BE MAILED OR DELIVERED TO EACH PERSON RECEIVING A SET OF THE ORIGINAL BID OR QUOTATION DOCUMENTS. LSUHSC WILL NOT BE RESPONSIBLE FOR ANY OTHER EXPLANATION OR INTERPRETATION OF THE DOCUMENTS.

28. ACCEPTANCE OF BID: ONLY THE ISSUANCE OF A PURCHASE ORDER OR A SIGNED CONTRACT CONSTITUTES ACCEPTANCE ON THE PART OF LSUHSC.

29. ADHERENCE TO JCAHO STANDARDS: WHERE APPLICABLE, LSUHSC IS ACCREDITED BY THE JOINT COMMISSION ON ACCREDITATION OF HEALTHCARE ORGANIZATIONS AND AS SUCH ALL CONTRACTORS, SUBCONTRACTORS, AND VENDORS AGREE TO ADHERE TO THE APPLICABLE STANDARDS PROMULGATED BY THE COMMISSION.

30. PREFERENCE: IN ACCORDANCE WITH LOUISIANA REVISED STATUTES 39:1595, A PREFERENCE MAY BE ALLOWED FOR PRODUCTS MANUFACTURED, PRODUCED, GROWN, OR ASSEMBLED IN LOUISIANA OF EQUAL QUALITY. DO YOU CLAIM THIS PREFERENCE? YES _____ NO_____

SPECIFY THE LINE NUMBER (S) _____

SPECIFY LOCATION WITHIN LOUISIANA WHERE THIS PRODUCT IS MANUFACTURED, PRODUCED, GROWN OR ASSEMBLED _____

(NOTE: IF MORE SPACE IS REQUIRED, INCLUDE ON SEPARATE SHEET.)

DO YOU HAVE A LOUISIANA BUSNIESS WORK FORCE? YES _____ NO _____

IF SO, DO YOU CERTIFY THAT AT LEAST FIFTY PERCENT (50%) OF YOUR LOUISIANA WORKFORCE IS COMPRISED OF LOUISIANA RESIDENTS?

YES_____ NO_____

FAILURE TO SPECIFY ABOVE INFORMATION MAY CAUSE ELIMINATION FROM PREFERENCES.

PREFERENCES SHALL NOT APPLY TO SERVICE CONTRACTS.

31. SIGNATURE AUTHORITY. IN ACCORDANCE WITH L.R.S. 39:1594 (ACT 121), THE PERSON SIGNING THE BID MUST BE:

31.1. A CURRENT CORPORATE OFFICER, PARTNERSHIP MEMBER OR OTHER INDIVIDUAL SPECIFICALLY AUTHORIZED TO SUBMIT A BID AS REFLECTED IN THE APPROPRIATE RECORDS ON FILE WITH THE SECRETARY OF STATE; OR

31.2. AN INDIVIDUAL AUTHORIZED TO BIND THE VENDOR AS REFLECTED BY AN ACCOMPANYING CORPORATE RESOLUTION, CERTIFICATE OR AFFIDAVIT; OR

31.3. AN INDIVIDUAL LISTED ON THE STATE OF LOUISIANA BIDDER'S APPLICATION AS AUTHORIZED TO EXECUTE BIDS. BY SIGNING THE BID, THE BIDDER CERTIFIES COMPLIANCE WITH THE ABOVE.

PRICE SHEET

NUMBER : 005452 BIDDER:

OPEN DATE : 03/26/2010 TIME: 02:00 PM

UNLESS SPECIFIED ELSEWHERE SHIP TO:

Receiving Department
3010 Linwood Avenue
Shreveport LA 71130

Line No.	Description			Unit Price	Extended Amount
1	CS-LSU Medical Center - ARUBA 5000 Base 400 Restricted Regulatory Domain - US -- PLEASE SEE ATTACHMENT FOR SYSTEM TECHNICAL SPECIFICATIONS Specify brand, model bid(if applicable)	1.00	EA		
2	CS-LSU Medical Center - ARUBA Multi-Service Mobility Module Mark I 10X 1000Base-X SFP 2X 10GBase-X XFP O AP Support Specify brand, model bid(if applicable)	1.00	EA		
3	Next-Day Support for M3MK1-S 1 Year Specify brand, model bid(if applicable)	1.00	EA		
4	CS-LSU Medical Center - Access Point License 256 Access Point License Specify brand, model bid(if applicable)	1.00	EA		
5	ARUBA Care Support for Lic-256-AP 1 Year Specify brand, model bid(if applicable)	1.00	EA		
6	CS-LSU Medical Center - Pef License 1024 Users Specify brand, model bid(if applicable)	1.00	EA		
7	Support for LIC-Pef-1024 1 Year Specify brand, model bid(if applicable)	1.00	EA		

NUMBER : 005452 BIDDER:

OPEN DATE : 03/26/2010 TIME: 02:00 PM

UNLESS SPECIFIED ELSEWHERE SHIP TO:

Receiving Department
3010 Linwood Avenue
Shreveport LA 71130

Line No.	Description			Unit Price	Extended Amount
8	AC Power Cord North America Version Specify brand, model bid(if applicable) _____	1.00	EA	_____	_____
9	CS-LSU Medical Center - ARUBA 105 Wireless Access Point Dual Radio Specify brand, model bid(if applicable) _____	225.00	EA	_____	_____
10	CS-LSU Medical Center - ARUBA 105 Wireless Access Point Ceiling Mounting Kit Specify brand, model bid(if applicable) _____	225.00	EA	_____	_____

LSUHSC SHREVEPORT

WLAN TECHNICAL REQUIREMENTS

Contents

Solution Features

1.1 General

1.1.1 Centralized WLAN architecture with "thin" Access Point and centralized switch/controllers, and integrated network management

1.1.2 Wi-Fi Alliance Certification for 802.11 a/b/g

1.1.3 Self-contained, integrated, overlay solution, not requiring upgrades or enhancements to existing routers and switches

1.1.4 Chassis and box 1-1 and N+1 redundancy with under 20 seconds failover time

1.1.5 The same software, configurations and product functionality supported across all platforms in the product family proposed

1.1.6 Newly installed controllers automatically synchronized with the already existing controller(s), without requiring a separate network management server

1.2 Authentication & Encryption

1.2.1 Support the following:

1.2.1.1 MAC based authentication.

1.2.1.2 802.1X based authentication.

1.2.1.3 WPA2/AES link layer encryption.

1.2.1.4 WEP link layer encryption.

1.2.1.5 WPA/TKIP link layer encryption.

1.2.1.6 LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC authentication.

1.2.1.7 Integrated RADIUS termination for increased security and cryptographic offload. Must support EAP-PEAP and EAP-TLS using EAP-MSCHAPv2 or EAP-GTC.

1.2.2 Web-Based Authentication (e.g. WebAuth/Captive Portal):

1.2.2.1 Integrated into the controller/switch.

1.2.2.2 User name and password authentication, as well as support for token based authentication.

1.2.2.3 Option for simple logging of user name used for entry.

1.2.2.4 Facilitate process for non-IT staff to create temporary guest IDs and passwords to automatically age out / expire.

1.2.2.5 Ability to customize the pre-authentication network access rights beyond DHCP response (e.g. to allow PCs and MACs to finish network scripts and network boot ups),

1.2.2.6 API's for scripted control of these features from external system.

1.2.2.7 Airtime-based bandwidth contract for the guest SSID to preserve channel access for particular SSIDs. As an example, granting a higher percentage of airtime to employee SSIDs as opposed to guest SSIDs.

1.2.2.8 Packet-rate based bandwidth contract for individual guest users for increased control of guest traffic usage.

1.2.2.9 802.1X based guest access using a local database on the switch/controller that can be used to authenticate users.

1.2.2.10 Time-of-day / duration based access per guest user of increased control and security

1.2.2.11 Time-of-day availability of guest SSID for increased control and security

1.2.2.12 Secure tunneling via IPSec/GRE to a generic L3 switch/router (located in the DMZ) for ease of deployment and reduced cost

1.3 Access Points (APs)

1.3.1 802.11 a/b/g functionality certified by the Wi-Fi alliance.

1.3.2 Plenum rated with applicable certifications.

1.3.3 Able to be powered over 802.3af standard Power-over-Ethernet (PoE).

1.3.4 Auto-sensing 10/100 on the network port.

1.3.5 Auto-sensing 10/100/1000 on the network port for 802.11n APs.

1.3.6 Support 802.3af standard Power-over-Ethernet (PoE) capability on for 3x3 MIMO dual-radio operation at full power of the radios – and 2 spatial streams for the 802.11n capable APs

1.3.7 Support the use of 802.11n and MIMO technologies on 2.4GHz radios

1.3.8 Options for dual-band single-radio APs which can perform RF scanning on both bands while serving WLAN clients on one band.

1.3.9 Ceiling and/or wall mounting options.

1.3.10 Integral facility for security lockdown (e.g. Kensington lock-point)

1.3.11 Support out-of-the box, auto configuration across layer-2 and layer-3 networks without having to enter configuration information into the AP.

1.3.12 APs do not hold "hard configured" internal network information or certificates for authentication to the centralized switches unless this information is stored in a trusted platform module (TPM) integrated into the AP.

1.3.13 Minimum of 8 SSIDs and BSSIDs available on each AP.

1.3.14 Capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical "touch" and no additional cost.

1.3.15 Real time packet capture on the APs, without disconnecting clients

1.3.16 Internal and external antenna options.

1.3.17 Maximum device size 5.5 inches by 5.5 inches square.

1.3.18 Wi-Fi alliance 802.11n Draft 2.0 certified APs.

1.3.19 Auto-sensing 10/100/1000 on the network port.

1.3.20 Provide a 2nd Ethernet port in order to enable secure access for wired client devices as required, or to act as a backup connection to the network.

1.4 AP-to-Controller Communication

1.4.1 Use of industry standards-based (IEEE or IETF) tunneling protocols; specify standard that the tunneling mechanism is based on.

1.4.2 Option to encrypt control path between the AP and the controller via standards-based protocols; specify standard that the encryption mechanism is based on.

1.4.3 Centralized Encryption/De-encryption (e.g. on switch/controller in data center) to prevent wired eavesdropping on wireless user data and malicious attacks on APs

1.4.4 Optionally support distributed Encryption/De-encryption (e.g. on AP's) without the need for specialized hardware with support mixed mode operations from a single switch/controller.

1.4.5 Support secure connection (e.g. IPSEC/VPN) of APs to centralized switch over "untrusted" (e.g. public WAN) network transport – with data and control path encryption – without requiring external hardware and without requiring dedicated switch/controller.

1.4.6 Improve enterprise wide mobility by securing legacy devices with integrated client VPN and site-to-site VPN

1.4.7 Support policy based forwarding on the AP with integrated firewall for access control

1.5 AP Management

1.5.1 Automatic updates of firmware and software on all APs without user intervention.

1.5.2 Support discovery protocol from APs to find and sync with switch/controller, that works over routed and switched subnets and that does not require reconfiguration or features on routers or switches.

1.5.3 All AP configuration and service delivery information centrally managed and maintained via the switch/controller.

1.5.4 Centralized switch/controller provides an easy to use (template based) mechanism to support configuration of different groups of APs – without requiring a separate management interface.

1.5.5 AP management performed through the use of groups and profiles for ease of scalability and deployment.

1.6 RF Management

1.6.1 Enable ease of deployment and ongoing management with automatic adjustment of individual AP power and channel setting to maximize performance around other APs, limit the effects of interference (both 802.11 and non-802.11), and detect and correct any RF coverage holes.

1.6.2 Support DFS certified radios that can enable 14 additional 5GHz channels thereby increasing total WLAN capacity.

1.6.3 Prevent data loss with adaptive RF management that provides the capability to pause channel scanning / adjust RF scanning intervals based on application and load presence – including voice and video sessions (both multicast or unicast)

1.6.4 Dynamic load balancing to automatically distribute clients to the least loaded 802.11 channel and AP; load balancing must not require any client specific configurations or software.

1.6.5 APs that are used for WLAN access should continue to perform RF scanning for the purposes of dynamic RF management and wireless intrusion detection and prevention; however this scanning should not adversely affect data transmission for mission-critical applications (user-defined), voice (through active / in-active call recognition) and load (user-defined threshold) – in other words, APs should delay scanning under these

conditions until such time as resumption of scanning will not negatively impact these services.

1.6.6 Load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.

1.6.7 Traffic shaping capabilities to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software.

1.6.8 Capability to provide preferred access for "fast" clients over "slow" clients (11n vs. 11a/b/g, and 11g vs. 11b) in order to improve overall network performance.

1.6.9 Co-channel interference management in order to prevent adverse affects of operating multiple APs in the same channel while in close proximity thereby improving overall WLAN capacity by enabling the same 802.11 channel to be re-used at shorter distances (for instance within 2.4GHz band where 3 x 802.11 channels are available).

1.6.10 Ability to mitigate adjacent channel interference among the APs operating on "neighboring" channels

1.6.11 Ability to allocate / dedicate a slice of bandwidth for a particular SSID based on access class (video, voice, data, etc.)

1.6.12 System should support the above functions in real time and without the need to perform any network baselines or manually administered measurements and must be based on real RF information versus models in management systems.

1.7 Access Control

1.7.1 Security enforcement for wireless users through the use of a role-based, stateful firewall that can be directly integrated with the roles defined within existing authentication servers.

1.7.2 Dynamic, stateful (as defined by ICSA) access rights into the network once authenticated based on source, destination, and/or ports.

1.7.3 Capability to ensure privacy protection by preventing firewall and IP spoofing attacks, and enforcing TCP handshake

1.7.4 Access policies should provide for automatic capture of data and syslog of access rule triggers for audit and analysis.

1.7.5 Rules for access rights based on any combination of time, location, user identity, device identity, and extended attributes from the authentication database.

1.7.6 The firewall must be able to take action including allowing the traffic, denying the traffic, rejecting the traffic, routing the traffic, destination or source NAT the traffic, modify the QoS level of the traffic, and blacklist (remove from the network) the client for policy matches.

1.7.7 Centralized switch / controller should provide the capability to support dynamic role updates of users (e.g. full-access to quarantined) based on messages received from any type of external IDS through the use of an integrated syslog parser.

1.7.8 Integrate with NAC solutions through role based access control architecture

1.7.9 Centralized switch / controller should provide the capability to support dynamic role updates of users (e.g. full-access to quarantined) based on messages received from any type of external IDS and NAC systems through the use of an integrated XML API.

1.8 Intrusion Detection / Prevention

1.8.1 Automatic Rogue AP classification (from interfering APs) and automatic rogue AP containment without requiring dedicated APs to listen on the wired ports or any other manual procedure (e.g. support the use of hybrid APs (scan & serve) and dedicated sensors simultaneously)

1.8.2 Utilization of the same server / user interface for WIPS and WLAN data collection

1.8.3 Accurate and automatic method of classifying real Rogues (on network) versus interfering neighbor networks whether Rogues have encryption or not and without client software or upgrades to current network.

1.8.4 Automatic Ad-hoc network detection and containment

1.8.5 Detection of wireless bridges

1.8.6 Protection for Man-In-The-Middle and Honey-Pot attacks

1.8.7 Protection for denial of service attacks

1.8.8 Protection for MAC address spoofing

1.8.9 User-definable rate threshold detection and protection

1.8.10 Detection of active network scanning tools

1.8.11 Data/packet CRC and sequence error detection and prevention

1.8.12 Blacklisting of wireless user devices after failed authentication attempts for web based authentication and 802.1X authentication against user-defined thresholds

1.8.13 Blacklisting of wireless devices after wireless denial of service attack is detected from the wireless device

1.8.14 Blacklisting of wireless devices after firewall / ACL access rule violations are detected within the centralized switch / controller

1.8.15 Attack signatures based on Wireless Vulnerability and Exploits (WVE) database signatures.

1.8.16 Attack alerts must include a link to the WVE entry for that attack.

1.8.17 On-the-fly, update-able, user specified signatures for wireless security threats.

1.9 Mobility

1.9.1 The system must support L2 roaming capabilities across APs (terminated on the same and different controllers) with no special client-side software required.

1.9.2 The system must support L3 roaming capabilities across APs (terminated on the same and different controllers) with no special client-side software required.

1.9.3 The system must support Opportunistic Key Caching (OKC).

1.9.4 The system must support Pairwise Master Key (PMK) caching.

1.10 Quality of Service

1.10.1 The system must be WMM-certified by the Wi-Fi alliance.

1.10.2 Upstream and downstream packet tagging between AP and controller/switch using standard tagging mechanisms; specify exact tagging support.

1.10.3 Ability to enforce QoS tags for user data on the wire, between client and AP and between AP and WLAN controller

1.10.4 Prevent misuse of QoS rules with deep packet inspection and WMM queue enforcement for user data

1.10.5 Per user, per device, and per application/TCP-port prioritization.

1.10.6 Support advanced multicast features with multicast rate optimization, multi channel use and IGMP snooping

1.10.7 Support ability to dynamically adjust and optimize delivery method of video traffic (e.g. multicast vs. unicast) based on the number of associated clients who a subscribed to a multicast stream to improve overall video quality

1.10.8 Support reliable delivery of multicast traffic at 802.11n high throughput rates

1.10.9 Advanced voice QoS services that prioritize voice streams over data for mixed mode devices (e.g. traffic-based instead of SSID-based prioritization) for any authentication method used

1.10.10 Automatic call recognition of Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), VOCERA, Spectralink Voice Protocol (SVP) VoWLAN protocols

1.10.11 Dynamic voice-aware load balancing (call admission control) of SIP, SCCP, VOCERA, SVP VoWLAN protocols. This load balancing should preemptively move voice clients across APs while they are out-of-call in order to improve network performance

1.10.12 Battery-saving features such as proxy ARP for clients, multicast/broadcast filtering, large DTIM configurations, multicast/broadcast to unicast conversion integrated into the AP and controllers without requiring client side software components

1.11 Network Services

1.11.1 The system must support internal routing, bridging and spanning tree capabilities across its ports within the centralized switch/controller in order to enable ease of deployment and scalability.

1.11.2 Source NAT and destination NAT must be available for private address use.

1.11.3 Interfaces on the switch/controller must be able to be set for DHCP in order to operate where static IP addressing is not available.

1.11.4 An internal DHCP server for ease of deployment and scalability must be available and must be able to redistribute dynamically learned information such as DNS, WINS, and local DNS suffix entries in the DHCP response.

1.11.5 Support GRE and IPSEC tunnels between controllers and other GRE/IPSEC termination devices in order to enable secure site-to-site connections without requiring external hardware.

1.11.6 Support VLAN subnet management with multiple VLAN assignment (VLAN pooling) per SSID

1.11.7 Interoperable with any network access control software for all role-based policy enforcement features using syslog or XML APIs.

1.12 Management

1.12.1 Command line interface to control and manage all aspects of the system on the controller/switch.

1.12.2 SNMP v3

1.12.3 SSH must be supported and must be the default CLI access technology. Real-time configurable system changes, not requiring reboots or re-compilation to affect changes

1.12.4 Browser-based system for total solution management including: site planning, configuration, monitoring, troubleshooting, location, and reporting.

1.12.5 Support real-time live RF heatmap capabilities to eliminate the need for post-deployment manual measurements.

1.12.6 HTTPS must be supported and must be the default browser based interface access technology.

1.12.7 Single, unified management view to multiple controllers/switches and access points.

1.12.8 Single dashboard view of overall network, user, and security status

1.12.9 Administrative rights partitioning - different admins have different rights. At a minimum should be

1.12.9.1 full access – Full administrative privileges on the switch/controller.

1.12.9.2 read-only – Read only access on the switch/controller with no ability to modify the device configuration.

1.12.9.3 guest provisioning support – A limited interface that only allows for the provisioning of guest users.

1.12.10 Configuration and policy changes applied globally to all systems and APs from a single entry point.

1.12.11 Provide audit trail of administrative actions

1.12.12 Accurate, real-time location tracking of devices and users including rogue APs and security violators without separate location tracking or WIPS appliance

1.12.13 Visual RF maps of actual coverage and data rates without the requiring baselines of network signals and/or material modeling of facilities. Predictive site survey tool that works in conjunction with the Visual RF tool to plan the network based on modeling requirements.

1.12.14 Support for large scale deployments using browser based network management able to support multi-vendor networks from the same console.

1.12.15 The ability to keep greater than one year of data in the management tool for reporting/compliance reports.

1.12.16 APs can be updated to support wireless mesh capability without requiring a separate dedicated switch/controller or static radio configuration. Wireless mesh should support dynamic path routing for redundancy.

1.12.17 Wireless mesh capability should have options to support centralized encryption, wired traffic backhaul and local bridging.

1.12.18 Support advanced outdoor RF planning and management tools for accurate visualization of RF coverage in three dimensions.

1.12.19 Outdoor planning solution supports integration with Google Earth and capability to interface with external GIS systems.

1.12.20 APs can be upgraded from 802.11abg-only to 802.11abgn for cost-effective migration to 802.11n.

1.12.21 Enable multi-vendor WLAN management

1.12.22 Integrate with Remedy Services Desk to support single trouble ticket management across wired and wireless

1.12.23 Ability to schedule network configuration and software upgrades

1.12.24 Integrated compliance reporting functions

1.12.25 Ability to deliver real-time AP and user stats, and advanced search capabilities